Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2021) 45: 1180 – 1194
© TÜBİTAK
doi:10.3906/mat-2007-30

On self-orthogonality and self-duality of matrix-product codes over commutative rings

Abdulaziz DEAJIM*, **Mohamed BOUYE**
Department of Mathematics, King Khalid University, Abha, Saudi Arabia,

Received: 08.07.2020 • **Accepted/Published Online:** 24.03.2021 • **Final Version:** 20.05.2021

Abstract: Self-orthogonal codes and self-dual codes, on the one hand, and matrix-product codes, on the other, form important and sought-after classes of linear codes. Combining the two constructions would be advantageous. Adding to this combination the relaxation of the underlying algebraic structures to be commutative rings instead of fields would be even more advantageous. The current article paves a path in this direction. The authors study the problem of self-orthogonality and self-duality of matrix-product codes over a commutative ring with identity. Some methods as well as special matrices are introduced for the construction of such codes. A characterization of such codes in some cases is also given. Some concrete examples as well as applications to torsion codes are presented.

Key words: Commutative rings, matrix-product code, self-orthogonal codes, self-dual codes, torsion codes

1. Introduction

Besides being coding-theoretically very useful in their own right, Euclidean self-orthogonal and self-dual codes have proved to be interesting and usable in diverse areas of mathematics and its applications such as group theory, combinatorial designs, communication systems, and lattice theory (see [5, 6, 19, 20]). On the other hand, Blackmore and Norton, in their pioneering paper [2], introduced the important notion of matrix-product codes over finite fields. A matrix-product code utilizes a finite list of (input) codes of the same length to produce a longer code. The parameters and decoding capabilities of some of such codes were studied by many authors (see for instance [2, 9, 10]). Some authors also considered matrix-product codes and some of their properties over certain finite commutative rings (see for instance [1, 3, 4, 7]).

To connect the aforementioned concepts, one proper question on the topic is, "when can one construct a self-orthogonal or self-dual matrix-product code over a finite field?" To the best of the authors' knowledge, the work of Mankean and Jitman [15], which is a follow-up on [14], was the first published work that addresses this question. The aim of this paper is to consider the above question over an arbitrary commutative ring with unity (finite or infinite). Among other contributions, we generalize some results of [15] and, further, relax some of their requirements.

In order to give a self-contained description of the results, we give, in Section 2, the necessary preliminary definitions and results. It is assumed throughout the paper that the ring, R say, over which the codes are considered is a commutative ring with identity. In Section 3, sufficient conditions are given for a matrix-

*Correspondence: deajim@kku.edu.sa

2010 *AMS Mathematics Subject Classification:* 94B05, 94B15, 16S36

product code over R to be self-orthogonal (Theorems 3.1 and 3.3, and Corollary 3.5) or self-dual (Theorem 3.6). Theorem 3.8 introduces a condition under which we get a characterization of self-orthogonal and self-dual matrix-product codes over R. Theorem 3.4 gives a description of the dual of a matrix-product code over R, generalizing what is known over finite fields [2] and finite chain rings [1]. It is to be noted that Example 3.2 introduces a self-orthogonal MDS code over $\mathbb{Z}_{25}$. In Section 4, special matrices are introduced in order to be used in the construction of self-orthogonal and self-dual matrix-product codes with enhanced minimum distances. Some concrete examples are also given throughout the paper.

2. Preliminaries

Unless further assumptions are imposed, R denotes throughout this paper a commutative ring with identity 1 and $U(R)$ is its multiplicative group of units. To present our results under possibly broad assumptions, we choose not to put further restrictions on R unless they are really needed.

2.1. Linear Codes over R

Recall that *a code over R of length m* is a subset of R^m. Such a code is said to be *linear over R* if it is an R-submodule of R^m. A linear code C over R is said to be *free* if it is so as an R-module, where the cardinality of a (free) R-basis of C is called the *rank of C*. If C is a free linear code over R of length m and rank r, then a matrix $G \in M_{r\times m}(R)$ whose rows form an R-basis of C is called a *generating matrix* of C. In this case, a given element of C is precisely of the form xG for a unique $x \in R^r$.

Consider the Euclidean bilinear form (loosely called inner product) on R^m defined by $\langle x, y\rangle = x_1y_1 + \cdots + x_my_m$ for elements $x = (x_1, \dots, x_m)$ and $y = (y_1, \dots, y_m)$ of R^m. If C is a linear code over R of length m, define *the dual code $C^\perp$ of C* to be

$$C^\perp = \{x \in R^m \mid \langle x, c\rangle = 0 \text{ for all } c \in C\}.$$

It is easily checked that $C^\perp$ is a linear code over R as well. A linear code C over R is said to be *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$.

If C is a linear code over R of length m, recall that the Hamming distance on C is defined by

$$d(x, y) = |\{1 \le i \le m \mid x_i \ne y_i\}|$$

for $x = (x_1, \dots, x_m), y = (y_1, \dots, y_m) \in C$. Any distance in this paper is to mean the Hamming distance. The minimum distance of C is then defined to be

$$d(C) = \min\{d(x, y) \mid x, y \in C, x \ne y\}.$$

The Hamming weight is defined on C by $\text{wt}(x) = d(x, 0)$ for $x \in C$. So, for $x = (x_1, \dots, x_m) \in C$, $\text{wt}(x) = |\{1 \le i \le m \mid x_i \ne 0\}|$. It can be checked that $d(C) = \min\{\text{wt}(x) \mid x \in C, x \ne 0\}$. If C is free over R of length m, rank k, and minimum distance d, we say that C is an $[m, k, d]$*-linear code.*

2.2. Matrices over R

For positive integers s and l, with the assumption throughout that $s \le l$, we denote by $M_{s\times l}(R)$ the set of all $s \times l$ matrices with entries in R. For $A \in M_{s\times l}(R)$, denote by A^t the usual transpose of A. If the rows of $A \in M_{s\times l}(R)$ are linearly independent over R, we say that A *has full row rank*. For $\lambda_1, \ldots, \lambda_s \in R$, denote by $\mathrm{diag}(\lambda_1, \ldots, \lambda_s) \in M_{s\times s}(R)$ the diagonal matrix whose entry in position i, i is λ_i, and denote by $\mathrm{adiag}(\lambda_1, \ldots, \lambda_s) \in M_{s\times s}(R)$ the antidiagonal matrix whose entry in position $i, (s-i+1)$ is λ_i. A matrix $A \in M_{s\times s}(R)$ is *nonsingular* or *invertible* if and only if $\det(A) \in U(R)$. Note that if $A \in M_{s\times s}(R)$ and $AA^t = \mathrm{diag}(\lambda_1, \ldots, \lambda_s)$ or $\mathrm{adiag}(\lambda_1, \ldots, \lambda_s)$ with $\lambda_i \in U(R)$ for $i = 1, \ldots, s$, then both A and A^t are nonsingular, as classical properties of the determinant remain valid over commutative rings (see [16, I.D]).

2.3. Matrix-product codes over R

Let $C_1, \ldots, C_s$ be linear codes over R of length m and $A = (a_{i,j}) \in M_{s\times l}(R)$. Denote by $[C_1 \ldots C_s]\, A \subseteq M_{m\times l}(R)$ *the matrix-product code* over R in the sense of [2] (see also [1] and [7]); that is

$$[C_1 \ldots C_s]\, A = \{(c_1 \ldots c_s)A \,|\, c_i \in C_i,\, 1 \le i \le s\},$$

where $(c_1 \ldots c_s)$ is an $m \times s$ matrix whose ith column is $c_i \in C_i$ written in column form. The codes $C_1, \ldots, C_s$ are called the *input codes of* $[C_1 \ldots C_s]\, A$. Note that as $C_1, \ldots, C_s$ are linear over R, so is $[C_1 \ldots C_s]\, A$.

A typical codeword c of $[C_1 \ldots C_s]\, A$ is a matrix

$$c = (c_1 \ldots c_s)\, A = (x_{i,j}) \in M_{m\times l}(R)$$

with $x_{i,j} = \sum_{k=1}^{s} c_{i,k} a_{k,j}$, where $c_{i,k}$ is the ith component of c_k. As the two R-modules $M_{m\times l}(R)$ and R^{ml} are isomorphic, the length of the matrix-product code $[C_1 \ldots C_s]\, A$ is set to be ml. Besides, using the identification offered by the aforementioned isomorphism, we can also look at the codeword c as the ml-tuple

$$(x_{1,1}, \ldots, x_{1,l}, x_{2,1}, \ldots, x_{2,l}, \ldots, x_{m,1}, \ldots, x_{m,l}) =$$
$$\left(\sum_{k=1}^{s} c_{1,k}a_{k,1}, \ldots, \sum_{k=1}^{s} c_{1,k}a_{k,l}, \sum_{k=1}^{s} c_{2,k}a_{k,1}, \ldots, \sum_{k=1}^{s} c_{2,k}a_{k,l}, \ldots, \sum_{k=1}^{s} c_{m,k}a_{k,1}, \ldots, \sum_{k=1}^{s} c_{m,k}a_{k,l}\right) \in R^{ml}.$$

Now, on $M_{m\times l}(R)$ we consider the bilinear form $\langle A, B\rangle^* = \mathrm{trace}(AB^t) = \sum_{i=1}^{m}\sum_{j=1}^{l} a_{i,j}b_{i,j}$ for $A = (a_{i,j})$ and $B = (b_{i,j})$. It can be checked easily that for codewords $c, c' \in [C_1 \ldots C_s]\, A$ looked at either as elements of $M_{m\times l}(R)$ or as elements of R^{ml}, we have $\langle c, c'\rangle^* = \langle c, c'\rangle$, where $\langle .\,, .\rangle$ is the Euclidean bilinear form defined in Section 2.1. So, we may use either form interchangeably to define the dual of a matrix-product code.

If $I_s \in M_{s\times s}(R)$ is the identity matrix, we denote the matrix-product code $[C_1 \ldots C_s]\, I_s$ by $[C_1 \ldots C_s]$. If $A = (a_{i,j}) \in M_{s\times l}(R)$ is of full row rank and C_i is a free linear code over R of length m, rank r_i, and a generating matrix $G_i \in M_{r_i\times m}(R)$ for $i = 1, \ldots, s$, respectively, it is known that $[C_1 \ldots C_s]\, A$ is free of rank $r = \sum_{i=1}^{s} r_i$ with a generating matrix $(a_{i,j}G_i) \in M_{r\times lm}(R)$.

3. Self-orthogonal and self-dual matrix-product codes

The following two theorems give sufficient conditions for a matrix-product code to be self-orthogonal.

Theorem 3.1 *Let $A = (a_{i,j}) \in M_{s\times l}(R)$ be such that $AA^t = diag(\lambda_1, \ldots, \lambda_s)$ for some $\lambda_1, \ldots, \lambda_s \in R$. Suppose that $C_1, \ldots, C_s$ are linear codes over R of the same length such that, for $i = 1, \ldots, s$, C_i is self-orthogonal whenever $\lambda_i \neq 0$. Then, $[C_1 \ldots C_s]\, A$ is self-orthogonal.*

Proof Let $c \in [C_1 \dots C_s]\, A$. In order to show that $c \in ([C_1 \dots C_s]\, A)^{\perp}$, we prove that $\langle c, c' \rangle = 0$ for any $c' \in [C_1 \dots C_s]\, A$. Let

$$c = (\textstyle\sum_{i=1}^{s} a_{i,1}c_i, \sum_{i=1}^{s} a_{i,2}c_i, \dots, \sum_{i=1}^{s} a_{i,l}c_i) \text{ and } c' = (\sum_{i=1}^{s} a_{i,1}c_i', \sum_{i=1}^{s} a_{i,2}c_i', \dots, \sum_{i=1}^{s} a_{i,l}c_i')$$

for $c_i, c_i' \in C_i$, $i = 1, \dots s$. Then we have

$$\begin{aligned}
\langle c, c' \rangle &= \sum_{i=1}^{s}\sum_{j=1}^{s} a_{i,1}a_{j,1}\ \langle c_i, c_j' \rangle + \sum_{i=1}^{s}\sum_{j=1}^{s} a_{i,2}a_{j,2}\ \langle c_i, c_j' \rangle + \cdots + \sum_{i=1}^{s}\sum_{j=1}^{s} a_{i,l}a_{j,l}\ \langle c_i, c_j' \rangle \\
&= (\sum_{j=1}^{s} a_{1,j}a_{1,j})\ \langle c_1, c_1' \rangle + \cdots + (\sum_{j=1}^{s} a_{1,j}a_{s,j})\ \langle c_1, c_s' \rangle \\
&\quad + (\sum_{j=1}^{s} a_{2,j}a_{1,j})\ \langle c_2, c_1' \rangle + \cdots + (\sum_{j=1}^{s} a_{2,j}a_{s,j})\ \langle c_2, c_s' \rangle \\
&\quad + \cdots \\
&\quad + (\sum_{j=1}^{s} a_{s,j}a_{1,j})\ \langle c_s, c_1' \rangle + \cdots + (\sum_{j=1}^{s} a_{s,j}a_{s,j})\ \langle c_s, c_s' \rangle.
\end{aligned}$$

Now, for each $i = 1, \dots s$, $(\sum_{j=1}^{s} a_{i,j}a_{j,i})\langle c_i, c_i' \rangle = \lambda_i \langle c_i, c_i' \rangle = 0$, because either $\lambda_i = 0$ or $\langle c_i, c_i' \rangle = 0$ otherwise (since C_i is self-orthogonal in this case). On the other hand, $(\sum_{j=1}^{s} a_{i,j}a_{k,j})\langle c_i, c_k' \rangle = 0$ for $i \neq k$ as well, because $\sum_{j=1}^{s} a_{i,j}a_{k,j}$ is the entry of AA^t in position i,k, which is 0 by assumption. Hence, $\langle c, c' \rangle = 0$ as desired. □

Theorem 3.1 can also be generalized in a different direction as follows.

Theorem 3.2 *Let $A \in M_{s_1 \times l}(R)$ and $B \in M_{s_2 \times l}(R)$ be such that AA^t and BB^t are diagonal and every row of A is orthogonal to every row of B. Then, for any self-orthogonal codes $C_1, \dots, C_{s_1}$ and $C_1', \dots, C_{s_2}'$ over R of the same length m, the matrix-product code $\mathcal{C} = [C_1 \dots C_{s_1} C_1' \dots C_{s_2}'] \begin{pmatrix} A \\ B \end{pmatrix}$ is self-orthogonal.*

Proof let $x, y \in \mathcal{C}$. So, there are $x_i, y_i \in C_i$ and $x_j', y_j' \in C_j'$ for $i = 1, \dots, s_1$ and $j = 1, \dots, s_2$ such that $x = (x_1 \dots x_{s_1} x_1' \dots x_{s_2}') \begin{pmatrix} A \\ B \end{pmatrix}$ and $y = (y_1 \dots y_{s_1} y_1' \dots y_{s_2}') \begin{pmatrix} A \\ B \end{pmatrix}$. Let $AA^t = \mathrm{diag}(\lambda_1, \dots, \lambda_{s_1})$, $BB^t = \mathrm{diag}(\beta_1, \dots, \beta_{s_2})$, $x_i = (x_{1,i} \dots x_{m,i})^t$, $y_i = (y_{1,i} \dots y_{m,i})^t$, $x_j' = (x_{1,j}' \dots x_{m,j}')^t$, and

$y'_j = (y'_{1,j} \ldots y'_{m,j})^t$ for $i = 1, \ldots, s_1$ and $j = 1, \ldots, s_2$. We then have

$$\begin{aligned}
\langle x, y\rangle &= \mathrm{tr}\,(xy^t)\\
&= \mathrm{tr}\left((x_1 \ldots x_{s_1} x'_1 \ldots x'_{s_2}) \begin{pmatrix} A \\ B \end{pmatrix} (A^t\ B^t)\,(y_1 \ldots y_{s_1} y'_1 \ldots y'_{s_2})^t\right)\\
&= \mathrm{tr}\left((x_1 \ldots x_{s_1} x'_1 \ldots x'_{s_2}) \begin{pmatrix} AA^t & 0 \\ 0 & BB^t \end{pmatrix} (y_1 \ldots y_{s_1} y'_1 \ldots y'_{s_2})^t\right)\\
&= \mathrm{tr}\left(\begin{pmatrix} \lambda_1 x_{1,1} & \ldots & \lambda_{s_1} x_{1,s_1} & \beta_1 x'_{1,1} & \ldots & \beta_{s_2} x'_{1,s_2} \\ \vdots & & \vdots & \vdots & & \vdots \\ \lambda_1 x_{m,1} & \ldots & \lambda_{s_1} x_{m,s_1} & \beta_1 x'_{m,1} & \ldots & \beta_{s_2} x'_{m,s_2} \end{pmatrix} \begin{pmatrix} y_{1,1} & \ldots & y_{m,1} \\ \vdots & & \vdots \\ y_{1,s_1} & \ldots & y_{m,s_1} \\ y'_{1,1} & \ldots & y'_{m,1} \\ \vdots & & \vdots \\ y'_{1,s_2} & \ldots & y'_{m,s_2} \end{pmatrix}\right)\\
&= \mathrm{tr}\begin{pmatrix} \sum_{i=1}^{s_1} \lambda_i x_{1,i} y_{1,i} + \sum_{j=1}^{s_2} \beta_j x'_{1,j} y'_{1,j} & \ldots & * \\ \vdots & \ddots & \vdots \\ * & \ldots & \sum_{i=1}^{s_1} \lambda_i x_{m,i} y_{m,i} + \sum_{j=1}^{s_2} \beta_j x'_{m,j} y'_{m,j} \end{pmatrix}\\
&= \lambda_1 \sum_{i=1}^{m} x_{i,1} y_{i,1} + \cdots + \lambda_{s_1} \sum_{i=1}^{m} x_{i,s_1} y_{i,s_1} + \beta_1 \sum_{i=1}^{m} x'_{i,1} y'_{i,1} + \cdots + \beta_{s_2} \sum_{i=1}^{m} x'_{i,s_2} y'_{i,s_2}\\
&= \lambda_1 \langle x_1, y_1\rangle + \cdots + \lambda_{s_1} \langle x_{s_1}, y_{s_1}\rangle + \beta_1 \langle x'_1, y'_1\rangle + \cdots + \beta_{s_2} \langle x'_{s_2}, y'_{s_2}\rangle\\
&= \lambda_1(0) + \cdots + \lambda_{s_1}(0) + \beta_1(0) + \cdots + \beta_{s_2}(0)\\
&= 0.
\end{aligned}$$

□

Remark 3.1 *1. Theorem 3.1 generalizes and relaxes the assumptions of [15, Theorem III.1] that R be a finite field and all the input codes free and self-orthogonal.*

2. Indeed, the process given in Theorem 3.2 can be mimicked for more than two vertically concatenated matrices with the same assumptions.

Example 3.2 *Let $C_1 = (1,7)\mathbb{Z}_{25}$ and $C_2 = (1,2)\mathbb{Z}_{25}$. It can be checked that C_1 and C_2 are $[2,1,2]$-linear codes over $\mathbb{Z}_{25}$, where C_1 is self-orthogonal and C_2 is not self-orthogonal. Let $A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$. Then A is not of full row rank and $AA^t = diag(20, 0)$. Nonetheless, it follows from Theorem 3.1 that the matrix-product code $[C_1 C_2]\,A$ is self-orthogonal. Moreover, it is a $[4,1,4]$-linear code over $\mathbb{Z}_{25}$ and thus is an MDS code.*

Theorem 3.3 *Let $A \in M_{s\times l}(R)$ be such that $AA^t = adiag(\lambda_1, \ldots, \lambda_s)$ for some $\lambda_1, \ldots, \lambda_s \in R$. Suppose that $C_1, \ldots, C_s$ are linear codes over R of the same length such that, for $i = 1, \ldots, s$, $C_i \subseteq C_{s-i+1}^{\perp}$ whenever $\lambda_i \neq 0$. Then, $[C_1\ \ldots\ C_s]\,A$ is self-orthogonal.*

Proof Similar to the proof of Theorem 3.1 with the obvious adjustments. □

Remark 3.3 *Theorem 3.3 generalizes and relaxes the assumptions of [15, Theorem III.4] that R be a finite field, all the input codes be free, and $C_i \subseteq C_{s-i+1}^{\perp}$ for all $i = 1, \ldots, s$.*

Example 3.4 *Let $C_1 = 10Z_{20} = \{0, 10\}$ and $C_2 = 4\mathbb{Z}_{20} = \{0, 4, 8, 12, 16\}$. It can be seen that $C_1^{\perp} = 2\mathbb{Z}_{20} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$, $C_2^{\perp} = 5\mathbb{Z}_{20} = \{0, 5, 10, 15\}$, and thus $C_1 \subseteq C_2^{\perp}$ and $C_2 \subseteq C_1^{\perp}$. Take $A = \begin{pmatrix} 0 & 2 & 0 & 4 \\ 0 & 4 & 2 & 0 \end{pmatrix}$. Then, $AA^t = adiag(8, 8)$. It then follows from Theorem 3.3 that both $[C_1 C_2]\, A$ and $[C_2 C_1]\, A$ are self-orthogonal. Indeed,*

$$[C_1 C_2]\, A = \{(0,0,0,0), (0,16,8,0), (0,12,16,0), (0,8,4,0), (0,4,12,0)\},$$

$$[C_2 C_1]\, A = \{(0,0,0,0), (0,8,0,16), (0,16,0,12), (0,4,0,8), (0,12,0,4)\},$$

and it can be checked that $\langle (a,b,c,d), (a',b',c',d') \rangle = 0$ and $\langle (e,f,g,h), (e',f',g',h') \rangle = 0$ for all $(a,b,c,d), (a',b',c',d') \in [C_1 C_2]\, A$, and $(e,f,g,h), (e',f',g',h') \in [C_2 C_1]\, A$. Thus,

$$[C_1 C_2]\, A \subseteq ([C_1 C_2]\, A)^{\perp} \text{ and } [C_2 C_1]\, A \subseteq ([C_2 C_1]\, A)^{\perp}.$$

The equality $([C_1 \ldots C_s]\, A)^{\perp} = [C_1^{\perp} \ldots C_s^{\perp}]\, (A^{-1})^t$ is well-known to hold if R is a finite field or a finite chain ring, C_i are free over R, and $A \in M_{s \times s}(R)$ is non-singular (see [1, 2] for instance). In Theorem 3.4 below, we show that this fact remains true over any commutative ring R without even assuming that the input codes are free over R.

Theorem 3.4 *Let $A \in M_{s \times s}(R)$ be non-singular and $C_1, \ldots, C_s$ linear codes of length m over R. Then, the dual of the matrix product code $[C_1 \ldots C_s]\, A$ is given by*

$$([C_1, \ldots, C_s]\, A)^{\perp} = [C_1^{\perp} \ldots C_s^{\perp}]\, (A^{-1})^t.$$

Proof We first show that $([C_1 \ldots C_s]\, A)^{\perp} \subseteq [C_1^{\perp} \ldots C_s^{\perp}]\, (A^{-1})^t$. Let $x = (x_1, \ldots, x_s) \in ([C_1 \ldots C_s]\, A)^{\perp}$ with $A = (a_{i,j})$. Note that $x_i \in R^m$ for every i. Then, $\langle x, c \rangle = 0$ for every $c \in [C_1 \ldots C_s]\, A$. Then we have, for every $j = 1, \ldots, s$ and every $c_j \in C_j$,

$$\begin{aligned} 0 &= \langle (x_1, \ldots, x_s), (\sum_{j=1}^{s} a_{j,1} c_j, \ldots, \sum_{j=1}^{s} a_{j,s} c_j) \rangle \\ &= \sum_{i=1}^{s} \langle x_i, \sum_{j=1}^{s} a_{j,i} c_j \rangle. \end{aligned}$$

For a fixed j, apply the above equality to all codewords of $[C_1 \ldots C_s]\, A$ of the form $(c_1, \ldots, c_j, \ldots, c_s)\, A$ with $c_i = 0$ for $i \neq j$ and c_j running over all codewords of C_j to get

$$0 = \sum_{i=1}^{s} \langle x_i, a_{j,i} c_j \rangle = \sum_{i=1}^{s} \langle a_{j,i} x_i, c_j \rangle = \langle \sum_{i=1}^{s} a_{j,i} x_i, c_j \rangle.$$

It follows that $\sum_{i=1}^{s} a_{j,i} x_i \in C_j^{\perp}$. Doing this for every $j = 1, \ldots, s$, we get $(x_1, \ldots, x_s)\, A^t \in [C_1^{\perp}, \ldots, C_s^{\perp}]$, which yields that $x = (x_1, \ldots, x_s) \in [C_1^{\perp}, \ldots, C_s^{\perp}]\, (A^{-1})^t$.

Conversely, we show that $[C_1^\perp \dots C_s^\perp]\,(A^{-1})^t \subseteq ([C_1 \dots C_s]\,A)^\perp$. For $x \in [C_1^\perp \dots C_s^\perp]\,(A^{-1})^t$, we have $x = (x_1, \dots, x_s) = (c_1^\perp, \dots, c_s^\perp)\,(A^{-1})^t$, where $c_i^\perp \in C_i^\perp$ for $i = 1, \dots, s$. It then follows that $(x_1, \dots, x_s)\,A^t = (c_1^\perp, \dots, c_s^\perp)$ and, thus, $\sum_{i=1}^s a_{j,i}x_i = c_j^\perp \in C_j^\perp$ for every $j = 1, \dots, s$. This means that, for any fixed j and all $y_j \in C_j$,

$$0 = \langle \sum_{i=1}^s a_{j,i}x_i, y_j \rangle = \sum_{i=1}^s \langle a_{j,i}x_i, y_j \rangle = \sum_{i=1}^s \langle x_i, a_{j,i}y_j \rangle.$$

Doing this process for every $j = 1, \dots, s$ yields that $\sum_{i=1}^s \langle x_i, \sum_{j=1}^s a_{j,i}y_j \rangle = 0$ for all $y_j \in C_j$. So,

$$0 = \langle (x_1, \dots, x_s), (\sum_{j=1}^s a_{j,1}y_j, \dots, \sum_{j=1}^s a_{j,s}y_j) \rangle$$

for all $y_j \in C_j$, $j = 1, \dots, s$. Thus, $\langle x, c \rangle = 0$ for every $c \in [C_1 \dots C_s]\,A$ and, hence, $x \in ([C_1 \dots C_s]\,A)^\perp$. □

Corollary 3.5 *Keep the assumptions of Theorem 3.4, and assume further that A is orthogonal (i.e. $A = (A^{-1})^t$). Then,*

1. $([C_1 \dots C_s]\,A)^\perp = [C_1^\perp \dots C_s^\perp]\,A$.
2. *If C_i is self-orthogonal for each $i = 1, \dots, s$, then so is $[C_1 \dots C_s]\,A$.*
3. *If C_i is self-dual for each $i = 1, \dots, s$, then so is $[C_1 \dots C_s]\,A$.*
4. *If $C_i^\perp \subseteq C_i$ for each $i = 1, \dots, s$, then $([C_1 \dots C_s]\,A)^\perp \subseteq [C_1 \dots C_s]\,A$.*

Proof Direct consequences of applying the formula $([C_1, \dots, C_s]\,A)^\perp = [C_1^\perp \dots C_s^\perp]\,(A^{-1})^t$. □

Remark 3.5 *For part 4 of Corollary 3.5 to hold, orthogonality of A is sufficient but not necessary (see [8, Theorem 13]).*

Note that Corollary 3.5 gives, in particular, a sufficient condition for the self-duality of a matrix-product code. The following theorem gives another sufficient condition.

Theorem 3.6 *Let $A \in M_{s\times s}(R)$ be such that $AA^t = adiag(\lambda_1, \dots, \lambda_s)$ for $\lambda_1, \dots, \lambda_s \in U(R)$. Suppose that $C_1, \dots, C_s$ are linear codes of the same length over R such that $C_i = C_{s-i+1}^\perp$ for $i = 1, \dots, s$. Then, $[C_1 \dots C_s]\,A$ is self-dual.*

Proof Let $A = (a_{i,j})$. The containment $[C_1 \dots C_s]\,A \subseteq ([C_1 \dots C_s]\,A)^\perp$ follows from Theorem 3.3. It remains to show that $([C_1 \dots C_s]\,A)^\perp \subseteq [C_1 \dots C_s]\,A$. Let $x \in ([C_1 \dots C_s]\,A)^\perp$. Then, by Theorem 3.4, $x = [c_1', c_2', \dots, c_s'](A^{-1})^t$ for some $c_i' \in C_i^\perp$, $i = 1, \dots, s$. As $C_i = C_{s-i+1}^\perp$ for each $i = 1, \dots, s$, $C_{s-i+1} = C_{s-(s-i+1)+1}^\perp = C_i^\perp$ for each $i = 1, \dots, s$. Thus, $c_i' \in C_{s-i+1}$ for each $i = 1, \dots, s$. Let $\lambda_i' \in R$ be such that

$\lambda_i\lambda'_i = 1$ and set $e_{s-i+1} = \lambda'_i c'_i$ for $i = 1, \ldots, s$. It follows that $e_{s-i+1} \in C_{s-i+1}$ for $i = 1, \ldots, s$ since $\lambda'_i \in R$ and C_{s-i+1} is linear over R. As $AA^t = \mathrm{adiag}(\lambda_1, \ldots, \lambda_s)$, it follows that

$$(A^{-1})^t = (\lambda'_i a_{s-i+1,j}) = \begin{pmatrix} \lambda'_1 a_{s,1} & \lambda'_1 a_{s,2} & \ldots & \lambda'_1 a_{s,s} \\ \lambda'_2 a_{s-1,1} & \lambda'_2 a_{s-1,2} & \ldots & \lambda'_2 a_{s-1,s} \\ \vdots & \vdots & \ldots & \vdots \\ \lambda'_s a_{1,1} & \lambda'_s a_{1,2} & \ldots & \lambda'_s a_{1,s} \end{pmatrix}.$$

So, we have

$$\begin{aligned} x &= [c'_1, c'_2, \ldots, c'_s](A^{-1})^t \\ &= \left(\sum_{i=1}^{s} \lambda'_i a_{s-i+1,1} c'_i, \sum_{i=1}^{s} \lambda'_i a_{s-i+1,2} c'_i, \ldots, \sum_{i=1}^{s} \lambda'_i a_{s-i+1,s} c'_i\right) \\ &= \left(\sum_{i=1}^{s} a_{i,1} e_i, \sum_{i=1}^{s} a_{i,2} e_i, \ldots, \sum_{i=1}^{s} a_{i,s} e_i\right) \\ &= [e_1, e_2, \ldots, e_s]A \in [C_1 \ldots C_s]\, A. \end{aligned}$$

□

Remark 3.6 *Theorem 3.6 generalizes and relaxes the assumptions of [15, Corollary III.6] that R be a finite field, all the input codes be free, and $\lambda_1 = \cdots = \lambda_s$.*

Example 3.7 *Let $C = (1,7)\mathbb{Z}_{25}$. Then C is a linear self-dual code of length 2 over $\mathbb{Z}_{25}$. Indeed, for $a, b \in Z_{25}$, $\langle (a, 7a), (b, 7b)\rangle = ab(1 + 49) = 0$. So, $C \subseteq C^{\perp}$. On the other hand, for $(x, y) \in C^{\perp}$ and $(a, 7a) \in C$, $\langle (x, y), (a, 7a)\rangle = 0$ implies that $a(x + 7y) = 0$. Taking $a \in U(\mathbb{Z}_{25})$ yields $x + 7y = 0$ and, thus, $y = -7^{-1}x = 7x$. So, $(x, y) = (x, 7x) \in C$. Thus, $C^{\perp} \subseteq C$. Now, take $A = \begin{pmatrix} 1 & 7 \\ 7 & 1 \end{pmatrix}$. Then $AA^t = adiag(14, 14)$ and $14 \in U(\mathbb{Z}_{25})$. It then follows from Theorem 3.6 that $[C\, C]\, A$ is self-dual. As a side, it can be checked that $[C\, C]\, A$ contains no codeword of weight 1, while it contains, for instance, the codeword $\begin{pmatrix} 14 & 0 \\ 23 & 0 \end{pmatrix}$ which is of weight 2. So, the minimum distance of this matrix-product code is 2, which is the same as the minimum distance of C. On the other hand, C is free of rank 1, so its information rate is $1/2$. Similarly, $[C\, C]\, A$ is free of rank 2 and length 4, so its information rate is also $1/2$. Therefore, despite the fact that this matrix-product code caused doubling of the length of C and its cardinality, it nonetheless preserved the self-duality and both the minimum distance and the information rate of C.*

Our next goal is Theorem 3.8, in which we give a sufficient condition for the equivalence of self-orthogonality (resp. self-duality) of a matrix-product code and self-orthogonality (resp. self-duality) of its input codes.

Lemma 3.7 *Let $A = (a_{i,j}) \in M_{s\times s}(R)$ be non-singular and $C_1, \ldots, C_s$ linear codes of the same length over R. Then $[C_1 \ldots C_s]\, A = [C_1 \ldots C_s]$ if either of the following holds:*

1. *$C_1 \subseteq C_2 \subseteq \cdots \subseteq C_s$ and A is upper triangular.*

2. *$C_s \subseteq C_{s-1} \subseteq \cdots \subseteq C_1$ and A is lower triangular.*

3. *A is diagonal.*

4. *$C_1 = C_2 = \cdots = C_s$.*

Proof

1. Suppose that $C_1 \subseteq C_2 \subseteq \cdots \subseteq C_s$ and A is upper triangular. Then $a_{i,j} = 0$ for $i > j$. Moreover, $a_{j,j} \in U(R)$ for all $j = 1, \ldots, s$ since A is nonsingular. It follows that

$$[C_1 \ldots C_s]\, A = [a_{1,1}C_1, a_{1,2}C_1 + a_{2,2}C_2, \ldots, a_{1,s}C_1 + a_{2,s}C_2 + \cdots + a_{s,s}C_s].$$

Since $a_{1,1} \in U(R)$ and C_1 is linear, $a_{1,1}C_1 = C_1$. Similarly, $a_{2,2}C_2 = C_2$. Since $C_1 \subseteq C_2$ and C_2 is linear, $a_{1,2}C_1 \subseteq C_2$. It follows that $a_{1,2}C_1 + a_{2,2}C_2 = a_{1,2}C_1 + C_2 = C_2$. We continue in this manner to get that $a_{1,j}C_1 + a_{2,j}C_2 + \cdots + a_{j,j}C_j = C_j$ for all $j = 1, \ldots, s$. Thus, $[C_1 \ldots C_s]\, A = [C_1 \ldots C_s]$ as claimed.

2. If $C_s \subseteq C_{s-1} \subseteq \cdots \subseteq C_1$ and A is lower triangular, the proof is similar to case 1 above with the obvious adjustments.

3. Suppose that A is diagonal. So, $a_{i,j} = 0$, for all $i \neq j$, and $a_{j,j} \in U(R)$, for all $j = 1, \ldots, s$ (since A is non-singular). It follows that

$$[C_1 \ldots C_s]\, A = [a_{1,1}C_1 \ldots a_{s,s}C_s] = [C_1 \ldots C_s]$$

because $a_{j,j}C_j = C_j$, as $a_{j,j} \in U(R)$ and C_j is linear for every $j = 1, \ldots, s$.

4. Let $x \in [C \ldots C]\, A$. So, $x = (c_1 \ldots c_s)\, A$ for some $c_1, \ldots, c_s \in C$. By definition, we have $x = (\sum_{i=1}^{s} a_{i,1}c_i, \ldots, \sum_{i=1}^{s} a_{i,s}c_i)$. As $\sum_{i=1}^{s} a_{i,j}c_i \in C$ for all $j = 1, \ldots, s$, $x \in [C \ldots C]$ and, thus, $[C \ldots C]\, A \subseteq [C \ldots C]$. Conversely, let $x \in [C \ldots C]$. Applying the previous argument to A^{-1}, we have $[C \ldots C]\, A^{-1} \subseteq [C \ldots C]$. Now, $xA^{-1} \in [C \ldots C]\, A^{-1} \subseteq [C \ldots C]$. Hence, $x \in [C \ldots C]\, A$ and, therefore, $[C \ldots C] \subseteq [C \ldots C]\, A$.

□

Theorem 3.8 *Let $A \in M_{s\times s}(R)$ be non-singular and $C_1, \ldots, C_s$ linear codes of the same length over R such that $[C_1 \ldots C_s]\, A = [C_1 \ldots C_s]$. Then,*

1. *$[C_1 \ldots C_s]\, A$ is self-orthogonal if and only if $C_1, \ldots, C_s$ are all self-orthogonal.*

2. *$[C_1 \ldots C_s]\, A$ is self-dual if and only if $C_1, \ldots, C_s$ are all self-dual.*

Proof Assume that $[C_1 \ldots C_s]\, A = [C_1 \ldots C_s]$. Note that $[C_1 \ldots C_s] = [C_1 \ldots C_s]\, I_s$. By Theorem 3.4, we have

$$([C_1 \ldots C_s]\, A)^{\perp} = ([C_1 \ldots C_s]\, I_s)^{\perp} = [C_1^{\perp} \ldots C_s^{\perp}]\, (I_s^{-1})^t = [C_1^{\perp} \ldots C_s^{\perp}].$$

So, $[C_1 \ldots C_s]\, A$ is self-orthogonal (resp. self-dual) if and only if $[C_1 \ldots C_s] \subseteq [C_1^{\perp} \ldots C_s^{\perp}]$ (resp. $[C_1 \ldots C_s] = [C_1^{\perp} \ldots C_s^{\perp}]$). The claimed conclusion is now obvious. □

Corollary 3.9 *Let $A \in M_{s\times s}(R)$ be non-singular and $C_1, \ldots, C_s$ linear codes of the same length over R such that any of the conditions of Lemma 3.7 holds. Then,*

1. *$[C_1 \ldots C_s]\, A$ is self-orthogonal if and only if $C_1, C_2, \ldots, C_s$ are all self-orthogonal.*
2. *$[C_1 \ldots C_s]\, A$ is self-dual if and only if $C_1, C_2, \ldots, C_s$ are all self-dual.*

Proof Apply Lemma 3.7 and Theorem 3.8. □

4. Applications

4.1. Corollaries

For a finite commutative Frobenius ring R and a full-row-rank matrix $A \in M_{s\times l}(R)$ and $i = 1, \ldots, s$, denote by C_{R_i} the code of length l over R generated by the upper i rows of A. For linear codes $C_1, \ldots, C_s$ of the same length over R with minimum distances $d_1, \ldots, d_s$, respectively, it was shown in [7] that the minimum distance d of the matrix-product code $[C_1 \ldots C_s]\, A$ satisfies:

$$d \geq \min\{d_i \delta_i\}_{1 \leq i \leq s}, \tag{4.1}$$

where $\delta_1, \ldots, \delta_s$ are the minimum distances of $C_{R_1}, \ldots, C_{R_s}$, respectively.

By a *regular* element of R, we mean an element which is not a zero divisor. Recall, in particular, that if R is finite, then every regular element of R is a unit.

In the following results, R remains a commutative ring with identity, except when the above inequality is needed, in which case we require R to be finite and Frobenius.

Lemma 4.1 *If the characteristic of R is k with either $k = 0$ or $k > 1$ is odd, then $2 = 2.1_R$ is regular.*

Proof Let R be of characteristic zero. If 2 is not regular, then there exists $a \in R$, $a \neq 0$, such that $2a = 0$. This means that the subring aR of R has characteristic 2, which is impossible since the characteristic of a ring and its subrings have to be the same. On the other hand, suppose that $k = 2n+1$ is the characteristic of R for some $n \in \mathbb{N}$. Note that $2 \neq 0$ as k is odd. If 2 is not regular, then there exists $a \in R$, $a \neq 0$, such that $2a = 0$. Since also $ka = 0$, we have $0 = ka - 2a = (k-2)a = (k-2).1_R\, a$. By the minimality of k, $(k-2).1_R \neq 0$ and so $(k-2).1_R$ is not regualr. As $2a = 0 = (k-2)a$, $(k-4)a = (k-4).1_R\, a = 0$. Similarly, $0 \neq (k-4).1_R$ is not regular. Repeating this process n times yeilds $(k-2n)a = (k-2n).1_R\, a = 0$. But $k - 2n = 1$; so $1_R\, a = a = 0$, a contradiction. □

Lemma 4.2 *Let R be as in Lemma 4.1 and $A = \begin{pmatrix} 1 & u & 1 \\ -1 & 0 & 1 \end{pmatrix}$ for some $u \in U(R)$. Then, $AA^t = diag(2+u^2, 2)$, $\delta_1 = 3$, and $\delta_2 = 2$.*

Proof It is straightforward to check that $AA^t = \mathrm{diag}(2+u^2, 2)$. As $C_{R_1} = R(1, u, 1)$, an element of C_{R_1} is of the form $(\alpha, \alpha u, \alpha)$ for some $\alpha \in R$. Suppose that $\mathrm{wt}(\alpha, \alpha u, \alpha) = 1$. It is clearly impossible to have this assumption with $\alpha \neq 0$. But if $\alpha = 0$, then $(\alpha, \alpha u, \alpha) = (0, 0, 0)$, which is impossible as well. So, there is no $\alpha \in R$ such that $\mathrm{wt}(\alpha, \alpha u, \alpha) = 1$. Similarly, suppose that $\mathrm{wt}(\alpha, \alpha u, \alpha) = 2$. It is obvious that α cannot be zero. But if $\alpha \neq 0$, then we have $\alpha u = 0$, a contradiction. So, there is no $\alpha \in R$ such that $\mathrm{wt}(\alpha, \alpha u, \alpha) = 2$. Thus, $\delta_1 = 3$.

On the other hand, as $C_{R_2} = R(1,u,1) + R(-1,0,1)$, an element of C_{R_2} is of the form $(\alpha-\beta, \alpha u, \alpha+\beta)$ for some $\alpha, \beta \in R$. Suppose that $\mathrm{wt}(\alpha-\beta, \alpha u, \alpha+\beta) = 1$. Firstly, if $\alpha - \beta \neq 0$, then $\alpha u = 0$ (so $\alpha = 0$) and $\alpha+\beta = 0$. Since $\alpha = 0$ and $\alpha + \beta = 0$, we get $\beta = 0$. So, $\alpha - \beta = 0$, a contradiction. Secondly, if $\alpha u \neq 0$, then $\alpha - \beta = \alpha + \beta = 0$. So, $2\alpha = 0$ and thus $\alpha = 0$ (by Lemma 4.1). So, $\alpha u = 0$, a contradiction. Thirdly, if $\alpha + \beta \neq 0$, then $\alpha u = 0$ (so $\alpha = 0$) and $\alpha - \beta = 0$. Since $\alpha = 0$ and $\alpha - \beta = 0$, we get $\beta = 0$. So, $\alpha + \beta = 0$, a contradiction. So, there is no $\alpha, \beta \in R$ such that $\mathrm{wt}(\alpha-\beta, \alpha u, \alpha+\beta) = 1$. Thus, $\delta_2 \geq 2$. Since $(-1,0,1) \in C_{R_2}$, it must follow that $\delta_2 = 2$. □

Corollary 4.3 *Let R be as in Lemma 4.1. If there exist self-orthogonal linear codes C_1, C_2 of length m over R with respective minimum distances d_1, d_2, then there exists a self-orthogonal matrix-product code of length $3m$ over R with minimum distance d satisfying $d \geq min\{3d_1, 2d_2\}$.*

Proof Using the matrix A of Lemma 4.2, it follows from Theorem 3.1 that $[C_1C_2]\,A$ is self-orthogonal. Moreover, by (1), $d \geq \min\{3d_1, 2d_2\}$. □

Lemma 4.4 *Let R be such that -1 is a perfect square, say $-1 = u^2$ for some $u \in R$.*

1. *For $A = \begin{pmatrix} 1 & 0 & u \\ 0 & 1 & u \end{pmatrix}$, $AA^t = adiag(-1,-1)$ and $\delta_1 = \delta_2 = 2$.*
2. *If R is as in Lemma 4.1 and $B = \begin{pmatrix} 1 & u & 0 & 1 & u \\ u & 1 & u & 0 & 1 \end{pmatrix}$, then $BB^t = adiag(3u, 3u)$, $\delta_1 = 4$, and $\delta_2 = 3$.*

Proof Similar to the proof of Lemma 4.2 □

Corollary 4.5 *Let R be such that -1 is a perfect square. If there exist self-orthogonal linear codes C_1, C_2 of length m over R whose respective minimum distances are d_1, d_2 with $C_1 \subseteq C_2^{\perp}$ and $C_2 \subseteq C_1^{\perp}$, then*

1. *There exists a self-orthogonal matrix-product code C of length $3m$ over R, and if R is finite and Frobenius then the minimum distance d of C satisfies $d \geq min\{2d_1, 2d_2\}$.*
2. *If R is as in Lemma 4.1, then there exists a self-orthogonal matrix-product code C of length $5m$ over R, and if R is finite and Frobenius, then the minimum distance d of C satisfies $d \geq min\{4d_1, 3d_2\}$.*

Proof By respectively using the matrices A and B of Lemma 4.4, it follows form Theorem 3.3 that $[C_1C_2]\,A$ and $[C_1C_2]\,B$ are self-orthogonal of respective lengths $3m$ and $5m$. If R is finite and Frobenius, then it follows from (1) that d satisfies the indicated inequalities. □

Example 4.1 *It is a known fact that if p and q are odd primes, then -1 is a perfect square modulo pq if and only if -1 is a perfect square modulo each of p and q (see [17]). It is a also known that if p is congruent to 1 modulo 4, then -1 is a perfect square modulo p. Let p be a prime congruent to 1 modulo 4 and $R = \mathbb{Z}_{p^2}$. Then -1 is a perfect square in R. Let $x = (1,1,\ldots,1) \in R^p$, $y = (p,p,\ldots,p) \in R^p$, $C_1 = Rx$, and $C_2 = Ry$. Then, $d_1 = d_2 = p$, $C_1 \subseteq C_2^{\perp}$, and $C_2 \subseteq C_1^{\perp}$. Using the matrices A and B of Lemma 4.4, it follows from Corollary 4.5 that the matrix-product codes $[C_1C_2]\,A$ and $[C_1C_2]\,B$ are both self-orthogonal of lengths $3p$ and $5p$ and minimum distances satisfying $d \geq 2p$ and $d \geq 3p$, respectively.*

Lemma 4.6 *Let R be as in Lemma 4.1 in which -1 is a perfect square, say $-1 = u^2$ for some $u \in R$. Then for* $A = \begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix}$, $AA^t = adiag(2u, 2u)$, $\delta_1 = 2$, *and* $\delta_2 = 1$.

Proof Similar to the proof of Lemma 4.2 □

Corollary 4.7 *Let R be as in Lemma 4.6. If there exist linear codes C_1, C_2 of length m over R whose respective minimum distances are d_1, d_2 with $C_1 = C_2^\perp$ and $C_2 = C_1^\perp$, then there exists a self-dual matrix-product code C of length $2m$ over R, and if R is finite and Frobenius then the minimum distance d of C satisfies $d \geq min\{2d_1, d_2\}$.*

Proof Using the matrix A of Lemma 4.6, it follows from Theorem 3.6 that $[C_1C_2]\,A$ is self-dual. If R is finite and Frobenius, then it follows from (1) that d satisfies the indicated inequality. □

Remark 4.2 *Under the same assumptions on R of Lemma 4.6, a square matrix of any size, like the one in Lemma 4.6, can be constructed. If s is even, then*

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 & u \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & u & \dots & 0 & 0 \\ 0 & 0 & \dots & u & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots & \vdots \\ u & 0 & \dots & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in M_{s\times s}(R)$$

satisfies $AA^t = adiag(2u, 2u, \dots, 2u)$, $\delta_1 = \cdots = \delta_{s/2} = 2$, *and* $\delta_{s/2+1} = \cdots = \delta_s = 1$; *while if s is odd, then*

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & \dots & 0 & u \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 & u & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & u & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ u & 0 & \dots & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in M_{s\times s}(R)$$

satisfies $AA^t = adiag(2u, \dots, 2u, 1, 2u, \dots, 2u)$, $\delta_1 = \cdots = \delta_{(s-1)/2} = 2$, *and* $\delta_{(s+1)/2} = \cdots = \delta_s = 1$. *So, mimicking Corollary 4.7, Theorem 3.6 can be applied once there exist linear codes $C_1, \dots, C_s$ of length m over R whose respective minimum distances are $d_1, \dots, d_s$ with $C_i = C_{s-i+1}^\perp$, for $i = 1, \dots, s$, to get a self-dual matrix-product code of length sm and minimum distance d satisfying (if R is finite and Frobenius)*

$$d \geq \begin{cases} min\{2d_1, \dots, 2d_{s/2}, d_{s/2+1}, \dots, d_s\} & ; \ \textit{if } s \textit{ is even} \\ min\{2d_1, \dots, 2d_{(s-1)/2}, d_{(s+1)/2+1}, \dots, d_s\} & ; \ \textit{if } s \textit{ is odd.} \end{cases}$$

We end this subsection with the two tables below which give concrete examples highlighting the corollaries above. All input codes C_1 and C_2 below are self-dual (and, hence, self-orthogonal), which can be found in references [5, 11, 13]. The element -1 in the rings chosen is always a perfect square (see [5, Lemma 4.2] and [11, Lemma 3.1]). It was shown in [7] that if R is a finite commutative Frobenius ring, $A \in M_{s\times l}(R)$ is of full-row-rank, and $C_1, \ldots, C_s$ are free linear codes over R of ranks k_i for $i = 1, \ldots, s$, then the matrix-product code $[C_1 \ldots C_s]\, A$ is free of rank $\sum_{i=1}^{s} k_i$. Table 1 below concerns self-orthogonal matrix-product codes and Table 2 concerns self-dual matrix-product codes.

Table 1. self-orthogonal matrix-product codes.

R	C_1	C_2	$[C_1C_2]\,A$	Reason
$\mathrm{GR}(11^2, 2)$	$[12, 6, 6]$	$[12, 6, 7]$	$[36, 12, d \geq 14]$	Corollary 4.3
$\mathrm{GR}(11^2, 2)$, $\mathrm{GR}(5^3, 2)$	$[12, 6, 6]$	$[12, 6, 6]$	$[36, 12, d \geq 12]$	Corollary 4.5(1)
$\mathrm{GR}(11^2, 2)$, $\mathrm{GR}(5^3, 2)$	$[12, 6, 6]$	$[12, 6, 6]$	$[60, 12, d \geq 18]$	Corollary 4.5(2)
$\mathrm{GR}(5^3, 2)$, $\mathrm{GR}(3^4, 2)$, $\mathrm{GR}(3^2, 2)$	$[10, 5, 5]$	$[10, 5, 5]$	$[30, 10, d \geq 10]$	Corollary 4.5(1)
$\mathrm{GR}(5^3, 2)$	$[10, 5, 5]$	$[10, 5, 5]$	$[50, 10, d \geq 15]$	Corollary 4.5(2)
$\mathrm{GR}(3^2, 2)[x]/(x^2 - 3)$	$[8, 4, 5]$	$[8, 4, 5]$	$[24, 8, d \geq 10]$	Corollary 4.5(1)
$\mathbb{Z}_{25}$, $\mathrm{GR}(3^2, 2)$, $\mathrm{GR}(3^2, 2)[x]/(x^2 - 3)$	$[6, 3, 4]$	$[6, 3, 4]$	$[18, 6, d \geq 8]$	Corollary 4.5(1)
$\mathbb{Z}_{25}$	$[6, 3, 4]$	$[6, 3, 4]$	$[30, 6, d \geq 12]$	Corollary 4.5(2)
$\mathrm{GR}(3^2, 2)$	$[4, 2, 3]$	$[4, 2, 3]$	$[12, 4, d \geq 6]$	Corollary 4.5(1)

Table 2. self-dual matrix-product codes.

R	C_1	C_2	$[C_1C_2]\,A$	Reason
$\mathrm{GR}(11^2, 2)$	$[12, 6, 7]$	$[12, 6, 7]$	$[24, 12, d \geq 7]$	Corollary 4.7
$\mathrm{GR}(11^2, 2)$, $\mathrm{GR}(5^3, 2)$	$[12, 6, 6]$	$[12, 6, 6]$	$[24, 12, d \geq 6]$	Corollary 4.7
$\mathrm{GR}(5^3, 2)$, $\mathrm{GR}(3^4, 2)$, $\mathrm{GR}(3^2, 2)$	$[10, 5, 5]$	$[10, 5, 5]$	$[20, 10, d \geq 5]$	Corollary 4.7
$\mathrm{GR}(3^2, 2)[x]/(x^2 - 3)$	$[8, 4, 5]$	$[8, 4, 5]$	$[16, 8, d \geq 5]$	Corollary 4.7
$\mathbb{Z}_{25}$, $\mathrm{GR}(3^2, 2)$, $\mathrm{GR}(3^2, 2)[x]/(x^2 - 3)$	$[6, 3, 4]$	$[6, 3, 4]$	$[12, 6, d \geq 4]$	Corollary 4.7
$\mathrm{GR}(3^2, 2)$	$[4, 2, 3]$	$[4, 2, 3]$	$[8, 4, d \geq 3]$	Corollary 4.7

4.2. Torsion matrix-product codes over a finite commutative chain ring

In this subsection, we let R be a finite commutative chain ring, $\langle\gamma\rangle$ its maximal ideal, e the nilpotency index of γ, and $k = R/\langle\gamma\rangle$ the residual field of R. For $r \in R$, denote by $\overline{r}$ the reduction of r modulo $\langle\gamma\rangle$. Then, for $x = (r_1, \ldots, r_m) \in R^m$, denote by $\overline{x}$ the tuple $(\overline{r_1}, \ldots, \overline{r_m}) \in k^m$. For a code C over R, let $\overline{C}$ denote the code $\{\overline{x} \mid x \in C\}$ over k. Similarly, for $A = [a_{i,j}] \in M_{s\times l}(R)$, denote by $\overline{A}$ the matrix $[\overline{a_{i,j}}] \in M_{s\times l}(k)$. For a linear code C of length m over R and $0 \leq i \leq e-1$, the linear code $\mathrm{Tor}_i(C) = \overline{(C : \gamma^i)}$ over k is called the *i-torsion code associated to C* (see [18]), where $(C : \gamma^i) := \{x \in R^m \mid \gamma^i x \in C\}$.

Lemma 4.8 *[5, Lemma 5.1 and Theorem 5.2]*

1. *If C is a self-orthogonal code over R, then so is $Tor_i(C)$ over k for $i = 0, \ldots, \lfloor \frac{e-1}{2} \rfloor$.*

2. *If C is a self-dual code over R and e is odd, then $Tor_{\frac{e-1}{2}}(C)$ is self-dual over k.*

Corollary 4.9 *Let $A \in M_{s\times l}(R)$ be such that $AA^t = diag(\lambda_1,\dots,\lambda_s)$. If $C_1,\dots C_s$ are linear codes of the same length over R such that, for $j = 1,\dots,s$, C_j is self-orthogonal whenever $\lambda_j \in U(R)$, then $[Tor_i(C_1)\dots Tor_i(C_s)]\,\overline{A}$ is self-orthogonal for $i = 0,\dots,\lfloor\frac{e-1}{2}\rfloor$.*

Proof For any $i = 0,\dots,\lfloor\frac{e-1}{2}\rfloor$ and $j = 1,\dots,s$, it follows from part 1 of Lemma 4.8 that $\mathrm{Tor}_i(C_j)$ is self-orthogonal whenever $\overline{\lambda_j} \neq 0$ (equivalently, $\lambda_j \in U(R)$). Now the result follows from Theorem 3.1. □

Example 4.3 *Over the ring $\mathbb{Z}_4$, consider the linear codes $C_1 = (1,1,1,1)\mathbb{Z}_4 + (2,0,2,0)\mathbb{Z}_4$ and $C_2 = (1,1,1,1)\mathbb{Z}_4 + (0,2,0,2)\mathbb{Z}_4$. It is clear that both codes are self-orthogonal of length 4. Note that $\lfloor\frac{e-1}{2}\rfloor = 0$. So, for any matrix $A \in M_{s\times s}(\mathbb{Z}_4)$ such that $AA^t = diag(\lambda_1,\dots,\lambda_s)$ with $\lambda_1,\dots,\lambda_s \in U(\mathbb{Z}_4)$, we get (by Corollary 4.9) that for $j = 1,\dots,s$ and any values $i_j \in \{1,2\}$, the matrix-product code $[Tor_0(C_{i_1})\dots Tor_0(C_{i_s})]\,\overline{A} = [\overline{C_{i_1}}\dots\overline{C_{i_s}}]\,\overline{A}$ is self-orthogonal.*

Corollary 4.10 *Let $A \in M_{s\times s}(R)$ be non-singular. If e is odd and $C_1,\dots,C_s$ are linear codes of the same length over R, then $Tor_{\frac{e-1}{2}}([C_1\dots C_s]\,A)$ is self-dual over k if any of the following conditions holds ($i = 1,\dots,s$):*

1. *$C_i = C_{s-i+1}^{\perp}$ and $AA^t = adiag(\lambda_1,\dots,\lambda_s)$ with $\lambda_i \in U(R)$.*
2. *All C_i are self-dual, $C_1 \subseteq C_2 \subseteq \dots \subseteq C_s$, and A is upper triangular.*
3. *All C_i are self-dual, $C_s \subseteq C_{s-1} \subseteq \dots \subseteq C_1$, and A is lower triangular.*
4. *All C_i are self-dual and A is diagonal.*
5. *C_1 is self-dual and $C_1 = C_2 = \dots = C_s$.*

Proof By Theorem 3.6 (for part 1) and Corollary 3.9 (for the other parts), it follows that $[C_1\dots C_s]\,A$ is self-dual. Now, part 2 of Lemma 4.8 gives the desired conclusion. □

Example 4.4 *Over the ring $\mathbb{Z}_{125}$, let C be the self-dual $[6,3,4]$-linear code over $\mathbb{Z}_{125}$ generated by the matrix (see [12, Example 4.5]):*

$$G = \begin{pmatrix} 1 & 0 & 88 & 88 & 40 & 6 \\ 4 & 22 & 1 & 0 & 90 & 93 \\ 20 & 110 & 109 & 37 & 1 & 57 \end{pmatrix}.$$

Then, by part 5 of Corollary 4.10, the matrix-product code $Tor_1([\underbrace{C\dots C}_{s}]\,A)$ is self-dual, for any nonsingular matrix $A \in M_{s\times s}(\mathbb{Z}_{125})$.

Acknowledgment

The authors deeply thank the anonymous referee for the useful comments and suggestions, which improved the quality of the paper. They also extend their thanks to Patrick Solé for some useful discussions. M. Bouye expresses his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through General Research Project under grant number GRP/86/38.

References

[1] van Asch B. Matrix-product codes over finite chain rings. Applicable Algebra in Engineering, Communication and Computing 2008; 19: 39-49.

[2] Blackmore T, Norton G. Matrix-product codes over $\mathbb{F}_q$. Applicable Algebra in Engineering, Communication and Computing 2001; 12: 477-500.

[3] Boulagouaz M, Deajim A. Matrix-product codes over commutative rings and constructions arising from (σ, δ)-codes. Journal of Mathematics 2021; 2021. doi.org/10.1155/2021/5521067.

[4] Deajim A, Bouye M, Guenda K. The hulls of matrix-product codes over commutative rings and applications. Journal of Applied Mathematics and Computing 2020. doi.org/10.1007/s12190-020-01447-z

[5] Dougherty S, Kim J, Lin H. Constructions of self-dual codes over finite commutative chain rings. International Journal of Information and Coding Theory 2010; 1: 171-190.

[6] Dzhumalieva-Stova M, Bouyukliev I, Monev V. Construction of self-orthogonal codes for combinatorial designs. Problmes of Information Transmission 2012; 48: 250-258.

[7] Fan Y, Ling S, Liu H. Matrix-product codes over finite commutative Frobenius rings. Designs, Codes and Cryptography 2014; 71: 201-227.

[8] Galindo C, Hernando F, Ruano D. New quantum codes from evaluation and matrix-product codes. Finite Fields and Their Applications 2015; 36: 98-120.

[9] Hernando F, Lally K, Ruano D. Construction and decoding of matrix-product codes from nested codes. Applicable Algebra in Engineering, Communications and Computing 2009; 20: 497-507.

[10] Hernando F, Ruano D. Decoding of matrix-product codes. Journal of Algebra and Its Applications 2013; 12: 1250185.

[11] Kim J, Lee Y. Construction of MDS self-dual codes over Galois rings. Designs, Codes and Cryptography 2007; 45: 247-258.

[12] Lee H, Lee Y. Construction of self-dual codes over finite rings $\mathbb{Z}_{p^m}$. Journal of Combinatorial Theory, Series A 2008; 115: 407-422.

[13] Lu H, Dong X, Liu Z, Zhang M. Quantum codes derived from self-orthogonal codes over large finite rings. In: IEEE Conference Publications, 3rd ICISCE; China; 2016. pp. 514-518.

[14] Mankean T. Self-Orthogoanl Matrix Product Codes over Finite Fields. PhD Thesis, Silpakorn University, Thailand, 2016.

[15] Mankean T, Jitman S. Matrix-product constructions for self-othogonal linear codes. In: IEEE Conference Publications, 12th ICMSA; Indonesia; 2016. pp. 6-10.

[16] McDonald B. Linear Algebra over Commutative Rings. New York and Basel: Marcel Dekker Inc., 1984.

[17] Niven I, Zuckerman H, Montegomery H. An Introduction to the Theory of Numbers. 5th Edition: Wiley, 2004.

[18] Norton G, Sălăgean A. On the structure of linear and cyclic codes over a finite chain ring. Applicable Algebra in Engineering, Communication and Computing 2000; 10: 489-506.

[19] Pless V. A classification of self-orthogonal codes over $GF(2)$. Discrete Mathematics 1972; 3: 209-246.

[20] Wan Z-X. A characteristic property of self-orthogonal codes and its application to lattices. Bulletin of the Belgian Mathematical Society 1998; 5: 477-482.